Cisco CCNP Security

Implementing and Operating Cisco Security Core Technologies (350-701 SCOR)

This exam covers foundational and core knowledge areas required for Cisco network security engineers.

Security Concepts

- Threat intelligence and research
- Common vulnerabilities and exposures (CVE)
- Exploit kits
- Indicators of compromise (IOC)

Network Security

- Firewalls (ASA, Firepower, etc.)
- VPN technologies (site-to-site, remote access)
- Intrusion Prevention Systems (IPS)
- Content and web security
- Next-generation firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS)

Securing the Cloud

- Cloud computing concepts
- Cloud security concepts
- Cloud service models
- Cloud deployment models

Secure Access

- Identity management (ISE)
- Authentication, authorization, and accounting (AAA)
- BYOD and endpoint compliance
- Secure access controls (802.1X)

Endpoint Protection

- Endpoint protection platforms (EPP)
- Endpoint detection and response (EDR)
- Secure endpoint administration

Security Monitoring

- Network and endpoint telemetry
- Security monitoring tools
- Security analytics
- Incident response

Network Security Policies and Procedures

- Security policy elements and strategies
- Risk assessment and mitigation
- Security awareness and training

Concentration Exams (Choose One):

After completing the core exam, you choose one concentration exam that aligns with your career goals or specialization:

Implementing and Configuring Cisco Identity Services Engine (300-710 SISE)

- Cisco ISE architecture
- Policy enforcement
- Web authentication and guest services
- BYOD

Securing Networks with Cisco Firepower (300-710 SNCF)

- Firepower Threat Defense (FTD) configuration
- NGFW features
- Advanced malware protection (AMP)
- Firepower device management

Securing Email with Cisco Email Security Appliance (300-720 SESA)

- Cisco Email Security Appliance (ESA)
- Email security features
- Email encryption and decryption
- Email authentication

Securing the Web with Cisco Web Security Appliance (300-725 SWSA)

- Cisco Web Security Appliance (WSA)
- Web security features
- Web filtering and control
- Application visibility and control (AVC)

Implementing Secure Solutions with Virtual Private Networks (SVPN) (300-730 SVPN)

- o Secure VPN types

- o Remote access VPNs

- o Site-to-site VPNs

- o High availability VPNs

Automating and Programming Cisco Security Solutions (300-735 SAUTO)

- o Network programmability foundation

- o APIs and protocols

- o Cisco SD-WAN security features

- o Automation tools and workflows